FUTURIOM
FUTURE OF CLOUD TECH

Cloud Market Trend Report

API and Shift Left Security (With RSA Conference Wrap)

May 2023

FUTURIOM.COM

Highlights of This Report:

- **The RSA Conference (RSAC) in San Francisco was bigger than ever.** Nearly 50,000 people and 700 companies gathered to discuss ongoing cyberthreats and technology solutions in the industry.
- **Strong trends in the cybersecurity war include platform integration, application programming (APIs) security, shift left security, and artificial intelligence (AI).** The RSAC highlighted these new risks and challenges, along with potential solutions.
- **As cybersecurity tools expand, expertise and integration are big challenges.** Many organizations are struggling with new ways to integrate data analytics with a wide range of cybersecurity platforms to combat risk, as well as staffing to solve these problems.
- **A shift left security mindset will be needed to meld DevOps and SecOps.** To integrate security operations (SecOps) and development operations (DevOps) into so-call "DevSecOps," cyber pros will need to focus on securing application code and APIs.
- **Akamai's acquisition of Neosec just prior to the RSAC ratified the new need for API security.** This M&A acquisition highlights a technology gap in cybersecurity portfolios. The deal has elevated visibility of other API security companies, including Noname Security, Cequence, and Wib.
- **Expect more cybersecurity market consolidation with integration plays.** With hundreds of niche security tools in the market, expect more acquisitions in markets such as API security, secure access service edge (SASE), cloud access security broker (CASB), zero trust network access (ZTNA), and cloud security posture management (CSPM).
- **Companies mentioned in this report:** Cequence, HiddenLayer, Neosec (Akamai), Noname Security, Salt Security, Orca Security, SentinelOne, Wib, and Wiz.

API Security
The holistic way

Comprehensive API security can only be achieved with a holistic solution across code, testing and production.

One platform.
Complete API security.

- 91% of all web traffic runs through APIs
- 50% of APIs are unmanaged, undetected and unprotected
- APIs have become the #1 cyber attack surface

The Fusion Platform

A new era in API security

The Fusion platform is the only holistic solution on the market that delivers visibility, protection, and control across the entire API lifecycle, from code, through testing and into production. Wib's Fusion platform is purpose built to understand and interpret API and business logic and deliver insights on API-specific threats.

Fusion Discovery
View the entire API attack surface with an automated API inventory

Fusion Defense
Detect API security vulnerabilities across the entire API lifecycle

Fusion Analysis
Assess risk and business impact of APIs and prioritize remediation

Secure. Liberate. Innovate.

wib.com

Table of Contents

1. Introduction 4

2. The RSAC Recap: Takeaways and Areas to Watch 5

Key Trends We Are Watching 7
Integration Remains a Key Theme 8

3. A Deeper Dive into API and Shift left Security 10

Recent Breaches and What They Mean for Shift left and API Security 11

Threats and Solutions for API Security 11
- BOLA Attacks 11
- Injection Attacks 12
- API Misconfiguration Attacks 13
- Shadow and Zombie APIs 13

Shifting Left to Secure the Supply Chain 13

4. The AI Question 14

5. Appendix: Shift Left and API Cybersecurity Companies to Watch 15

1. Introduction: RSAC Bigger Than Ever

We recently attended the RSA Conference (RSAC), which I have been attending on and off since 1994. This iconic conference shows the cybersecurity boom remains in full swing, with nearly 50,000 people and 700 companies estimated to be in attendance.

The RSAC was founded in 1991 by Jim Bidzos, who in 1986 took over a struggling company known as RSA Data Security Inc. and transformed it into one of the world's most powerful cybersecurity companies. The key was developing an encryption toolkit that brought basic encryption techniques to the masses. One of RSA's first clients was the company that developed Lotus Notes, which was a communications suite acquired by IBM. RSA, the company, was acquired by EMC in 2006, which was then subsumed by Dell Technologies in 2016. RSA in 2020 was divested and taken private. Bidzos went on to become CEO of public company Verisign.

The RSAC, along with Black Hat, remains one of the top conferences for the cyber community to share information and technology. Attack threats are ever-increasing, and board-level awareness of cybersecurity threats continues to grow. But it's clear that after years and billions of dollars of investment, new approaches are still needed. Many security professionals continue to have gaps in visibility and would like more assistance in integrating their cyber approach.

New threats such as code-level threats, open-source software, and threats to APIs and AI are complicating the situation. Combine this with the view that organizations will have to keep a more careful eye on the security of their code and data in the cloud, and we have the beginning of long trend we are tracking, which we are calling shift left for cybersecurity.

Shift left is a term used by information technology (IT) developers and DevOps types to describe the drive to push more operational testing and cybersecurity technologies further up in the development cycle – or to the left if you imagine a chart showing the development cycle over time, progressing from left to right.

We expect the shift left cybersecurity mindset to permeate many layers of cloud infrastructure – networking, code, operating systems, and hardware down to the memory level. All this needs to happen to implement better security policy and techniques in the code that runs in the cloud.

The shift left will also be important for helping another topic causing waves at the RSAC: AI. AI is yet another advanced technology that will pressure the cybersecurity industry to catch up. Organizations are only beginning to assess the risks of AI tools and the implications for both code and data security.

This report will cover these key trends as well as a vision of how the shift left and API security markets will evolve.

- ***R. Scott Raynovich, Principal Analyst, Futuriom***

2. The RSAC Recap: Takeaways and Areas to Watch

With more than 600 companies gathering at RSAC, there is no shortage of solutions. The question: Where do you start?

The largest cybersecurity vendors are always adding products, and they support vast portfolios of solutions, but innovation typically emerges in the startup area. Cybersecurity continues to remain one of the more robust areas of venture capital (VC) investment. The pace has slowed a bit, along with the rest of the technology industry, but there is plenty of money to go around. VC funding for cybersecurity startups hit $18.5 billion in 2022, down from $30 billion in 2021, according to Momentum Cyber.

The race for better solutions has produced a mind-boggling number of technologies. Take a look at the vast number of acronyms in the cybersecurity market and you quickly run out of letters: They include advanced threat protection (ATP), cloud access security broker (CASB), cloud security posture management (CSPM), cloud native applications protection platform (CNAPP), data loss prevention (DLP), extended detection and response (XDR), firewall-as-a-service (FWaaS), intrusion detection system/intrusion prevention system (IDS/IPS), next-generation firewall (NGFW), software-defined wide-area networking (SD-WAN), secure web gateway (SWG), unified threat management (UTM), and zero trust network access (ZTNA).

That's just to name a few. Other areas, such as shift left security and secure access service edge (SASE), represent specific trends toward integration or general approaches in the industry. There are also important trends emerging in confidential computing and even quantum security protection. In Section 3 of this report, we'll highlight an area that's heating up: shift left security and API security.

We realize that reading about all the acronyms in this market can make you want to take a CNAPP. Ha! Our survey research indicates that network operations teams, cloud teams, and security operations teams are overwhelmed with tools and tasks and would like to consolidate some of these functions into more powerful platforms.

Here are a few of the quotes we saw and heard from RSAC 2023:

"We must accept that many jobs will disappear, many will change, and some will be created."

- ***Rohit Ghai, CEO of RSA Security, on the impact of AI on the cybersecurity industry***

(Source: PCmag.com)

"The threats will change all the time. Don't ever forget the advantage that you do have. You should know more about your business, your systems, your topology, your infrastructure than any attacker does. This is an incredible advantage."

- *Kevin Mandia, CEO of Mandiant (owned by Google)*

(Source: RSAC)

"APIs have become the Achilles' heel of cybersecurity and the new frontline of cyber attacks. As operations teams leverage AI in their business functions - most commonly via APIs - how do you ensure the integrity of your API ecosystem? We know these models hallucinate and make things up. Organisations need to adopt a 'shift left' mindset to API security and provide a single 'holistic' view of the entire API ecosystem to help DevSecOps teams combat the rising API security threat."

- *Chuck Herrin, CTO, Wib*

(Source: Futuriom interview)

"The future of warfare is going to be autonomous, with smaller systems that are enabled by AI, like one person controlling twenty planes. In World War I, we are getting the first tanks and the first motorized vehicles, but we still have the chevaliers with horses and sabers. What did the chevaliers say about motorized vehicles? We are going to use those motorized vehicles to get the horses to the front so that we could start the fight. We have to envision the future with AI and think how we are going to fight with AI."

- *Retired General Richard D. Clarke*

(Source: Futuriom interview)

"I hate the acronyms. There have always been lots of point solutions. None of them exist today -- that's because they all need to converge."

- *Avi Shua, Chief Innovation Officer and Cofounder at Orca Security*

(Source: Futuriom interview)

Key Trends We Are Watching

Prior to the RSAC, I highlighted the themes we were looking out for at the conference. In addition to doing the deep dive on API security for this report, we were watching trends and activity in the SASE market, CNAPPs, CSPM, shift left security, API security, and AI. Many of the cybersecurity vendors were pouncing on these themes. Let's look at some of the key developments in the market.

CNAPP and CSPM as Platform Integrators. These new areas focus on protecting cloud workloads, activity, and applications. CNAPP targets cloud-native applications that are developed and deployed using containers and microservices. It focuses on protecting the individual components of an application, rather than the infrastructure hosting it. Because they are focused on cloud workloads and data, they can serve as a natural place to adopt AI/machine learning (ML) and serve as central hubs for collecting and analyzing data as cybersecurity integration platforms.

Some highlights on CSPMs and CNAPPs:

- **Orca Security's** Avi Shua told us that rather than focus on the acronyms, security practitioners want an integrated approach to protecting data no matter where it is. "They want to find the exposed vulnerability," Shua told us. "You need a consolidation tool that can simplify this complex world." Orca falls into the CSPM category, but it focuses on many other use cases such as cloud workload protection, Kubernetes and container security, shift left security, API security, and others.

  At the RSAC, Orca announced full integration with Microsoft Azure OpenAI GPT-4. The integration builds on the ChatGPT implementation in the Orca Cloud Security platform announced in January, which Orca says makes it the first CNAPP to support GPT-4 through the Azure OpenAI Service.

- **SentinelOne and Wiz** announced a joint integration to expand CNAPP. When SentinelOne detects a runtime threat in a cloud server or container, it ingests relevant context from Wiz about the cloud resource, including vulnerabilities, misconfigurations, and exposed secrets. Both of these vendors are high-profile security vendors, so we think this partnership demonstrates the trend toward platform integration.

SASE vs. SSE (secure service edge). SASE is a framework that integrates network security and access controls into a single cloud-based platform for edge applications such as branch networking. This includes popular network security functions such as NGFW, FWaaS, ATP, SWG, and CASB (and much more). This approach is becoming more popular to secure networks with an overlay, and it's merging with ZTNA as remote work and the need for secure access to cloud-based services continue to grow.

The debate comes down to how much security inspection and enforcement happens on premises or in the cloud. SSE-focused vendors such as Zscaler deliver most of the functionality from the cloud. Traditional SASE vendors such as Versa and VMware (VeloCloud) advocate an

end-to-end hybrid approach. Recall that SASE emerged from the SD-WAN market as the software-based networking vendors integrated security functionality.

We expect the architectural rhetoric to grow among SASE and SSE vendors in the coming months. This is because 1) There are so many of them; and 2) As hybrid work and multicloud architectures expand, the need for distributed network security will expand.

Highlights in SASE and SSE from the RSAC:

- **Cato Networks**, provider of an integrated SASE platform delivered from the cloud, announced the addition of Cato Remote Browser Isolation (RBI) to its Cato SASE Cloud platform. This demonstrates the race by SASE providers to add features, and Cato, which recently added CASB, has proven to be one of the fast-moving SASE providers in this area.

- **Open Systems**' Managed SASE won a Global InfoSec Award presented by Cyber Defense Magazine (CDM). Its suite of integrated and unified network and network security functions is delivered as a 24/7 managed service.

Integration Remains a Key Theme

With so many cybersecurity technologies in the market, one of the recurring themes we have heard from cybersecurity practitioners is the growing need for consolidation and integration of many different cybersecurity and network functions.

Todd Hathaway, an executive security advisor, told World Wide Technology in a blog about the RSAC:

> *"Conversations with chief information security officers (CISOs) and security leaders revealed a common theme: Do more with fewer new tools and expand the platforms you already have. Chief Information Security Officers (CISOs) want to do more with fewer tools and in as many cases as possible, consolidate tools. However, if you walked the vendor expo, this may seem like a major contradiction; the number of new technology options was enormous."*

This is a theme stressed by Orca Security's Shua. In addition to hating acronyms, Shua told us security professionals are demanding integration of point solutions. "[The practitioners] don't want a dozen tools, it's too expensive and they can't manage it," said Shua. "They don't want all those tools. They want to understand the risks in the environment. The value comes in context. The market needs consolidation to provide meaningful context."

In the future, Shua believes that every organization will be multicloud in nature and will need cybersecurity capabilities that are cloud native and context aware.

It does appear that more integration and cooperation among security technology solutions will be needed across the spectrum, including coordination of data, network, cloud, and endpoint intelligence.

3. A Deeper Dive into API and Shift left Security

As we mentioned earlier, shift left is a term used by IT developers and DevOps types to describe the drive to push more operational testing and cybersecurity technologies further up in the development cycle – or to the left if you imagine a chart showing the development cycle over time, progressing from left to right.

The idea of shift left is that security code and policy can be implemented earlier in the development process, such as a zero-trust policy approach that verifies code from several vectors to stop threats before they are plugged in.

Shift left encompasses several areas, but the key elements include API security, securing business logic, and supply-chain security – ensuring that the code, APIs, and data platforms companies use are secure and in proper compliance. The idea of shift left is that security code and policy can be implemented earlier in the development process, such as a zero-trust policy approach that verifies code from several vectors to stop threats before they become part of the application fabric.

“Customers are waking up to the issue and saying they really need this capability,” said Mike O'Malley, Chief Marketing Officer (CMO) of Noname Security. “We'll see larger vendors getting into this one way or another. It's something that customers are worried about. The market is starting to wake up to it.”

As a demonstration of this growing need, the recent acquisition of Neosec by Akamai shows how larger cybersecurity companies are adopting shift left and API security to expand their portfolios.

"When we started Neosec a few years ago, everybody was using some kind of application security, but still abuses happen all the time," said Giora Engle, Cofounder and CEO of Neosec, in an interview with Futuriom in March. "When we hear there is a new cyber attack, today it involves applications and APIs, because so much infrastructure is built on top of APIs."

Mani Sundaram, Executive Vice President and General Manager, Security Technology Group, Akamai Technologies, said in a published release: "Enterprises expose full business logic and process data via APIs, which, in a cloud-based economy, are vulnerable to cyberattacks. Neosec's platform and Akamai's application security portfolio will allow customers to gain visibility into all APIs, analyze their behavior and protect against API attacks."

Futuriom believes Akamai’s acquisition represents the first in a series of deals in the API security space.

Recent Breaches and What They Mean for Shift left and API Security

Cybersecurity is a difficult game to win. Whether it’s an attack on a major bank, a government, or a local law firm, breaches are happening nearly every day. Lately, new attacks have surfaced in the API and code-security area.

Following is a recap of some key cybersecurity attacks focused on applications and what they mean for the shift left cybersecurity movement:

Type of API Attack	Description	Source
Cross-site scripting attack	Lego site BrickLink was found vulnerable to cross-site scripting and other well-understood types of attacks, intensifying scrutiny on API security.	Techtarget.com
Compromised API key access	A MailChimp data breach in 2022 saw attackers using compromised API keys to gain access to an account through which attackers were able to target finance and crypto clients. The attackers later launched a phishing campaign against the customers of those crypto clients.	Helpnetsecurity.com
Unauthorized attack of insecure API server	An API server attack on Australian telecom operator Optus in September of 2022 resulted in a breach of 9.8 million customer records, including driver's licenses, passports, and Medicare ID numbers, in addition to names, phone numbers, and email addresses.	Protocol.com
Unauthorized token access	The CircleCI CI/CD service disclosed that earlier this year, a customer's GitHub token was compromised, resulting in a major change in the way that tokens were managed in the system, which required revoking all Project API tokens.	CircleCI.com
Login API vulnerability	Security flaws were discovered in the implementation of the Open Authorization (OAuth) social-login feature used by the online travel agency Booking.com. This exposed the services	www.infosecurity-magazine.com

	to both large-scale account takeover (ATO) on customers' accounts and server compromise, but the security holes were patched before any known compromise.	
API vulnerabilities in automotive software	Security researcher Sam Curry discovered widespread flaws in the APIs for software in vehicles and automobiles. This enabled a single point of failure, such as exploiting user credentials or API keys to unlock valuable data, sometimes exploiting mobile apps.	samcurry.net

These instances demonstrate that code, applications, and APIs are increasing becoming the targets of attacks that can cripple production applications environments. As these attacks increase, specific technology will be needed to prevent them.

Threats and Solutions for API Security

So why the growing concern over API security? There are many different attack vectors in the API and code domains. As seen by the attacks above, different areas can be targeted, whether that's a company's process for managing APIs, the storing of security tokens, or weak authentication practices for access to code and data.

Let's look at some of the key types of attacks in the API and shift left landscape (special thanks to Wib's Chuck Herrin for detailing these for us).

BOLA Attacks

Broken Object-Level Authorization (BOLA) attacks occur when object-level references are altered in an API request. This allows attackers to gain access to unauthorized objects or data.

A typical API request might look like this:

(Get the <bank account information> where <user id 154>:

GET /api/bankaccount/user_id=154

In a BOLA attack, the attacker will modify the ID to a different reference to receive other user data:

GET /api/bankaccount/user_id=742

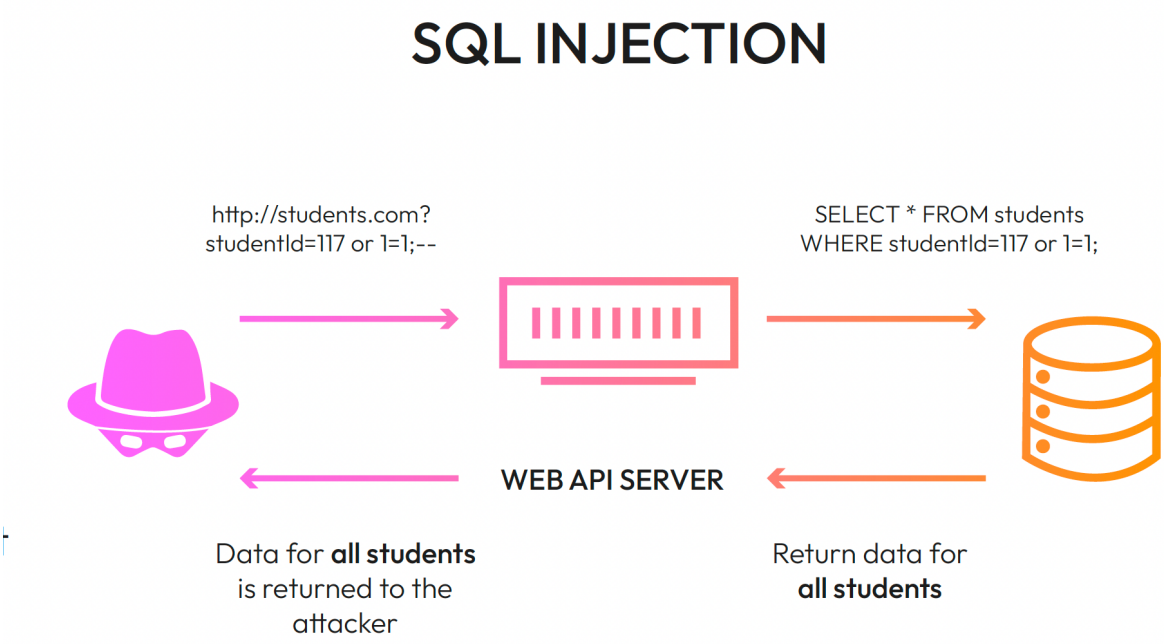
Typically this attack occurs when the attacker switches IDs and the correct authentication is not verified. Wib's Herrin points out that this is akin to going to pick up your car from the valet with

a claim ticket but forging the number on the claim ticket to take a nicer car (like a Ferrari, for example).

Solution: Organizations must take a multi-step process to prevent BOLA attacks. This includes implementing proper authentication mechanisms, validating user permissions, and using universally unique identifiers (UUIDs) to prevent attackers from guessing IDs. These systems should all be regularly tested.

Injection Attacks

Injection attacks occur when an attacker sends a malicious input, such as a string of code or data to a web application, to change the operation. The application can treat this injection as legitimate, triggering malicious consequences. Typical injection attacks include Structured Query Language (SQL) injection, NoSQL queries, operating system (OS) commands, or commands in protocols including Extensible Markup Language, Lightweight Directory Access Protocol (LDAP), and Object-Relational Mapping (ORM).



SQL injection attack (Source: Wib)

Solution: Developers need to properly validate and sanitize user input to prevent these types of common attacks. Typical techniques to prevent the attacks include developing safe APIs, validating incoming data, filtering character and data inputs, limiting the number of return records, and defining data types.

API Misconfiguration Attacks

Third-party misconfigurations occur when an API is exposed by a third-party and misconfigured, leading to a security vulnerability. For example, an API misconfiguration could allow an attacker to retrieve sensitive data without authentication or authorization (tokenization). Some of these types of attacks were included in our list of breaches above.

Solution: Businesses must log and monitor third-party API use and address misconfigurations. A key part of this process is using tools to gather an extensive view of APIs used in applications and data – both internal and external APIs.

Shadow and Zombie APIs

Shadow and zombie APIs refer to undocumented APIs existing in an organization's IT footprint. They may have been created by in-house developers or third parties and are no longer actively monitored. These APIs could still be used to access sensitive data or executive functions.

Solution: The most important precaution is to identify, monitor, and secure the shadow APIs to prevent breaches. Shadow APIs can be discovered with an inventory and audit program so that managers identify where the APIs exist and monitor them to prevent unauthorized use.

Shifting Left to Secure the Supply Chain

Shift left security is about more than just APIs. It also includes securing the development process, including monitoring code or environments such as containers and Kubernetes.

By shifting left, the security of code and testing can be implemented earlier in the development process to ensure better security. This might include critical tests such as Static Application Security Testing (SAST) to scan source code for security weaknesses. It can also include a variety of scans to take inventory and provide compliance for source-code libraries or container runtimes, for example.

Another key role in shift left is to minimize software supply chain risks. This means implementing a system that can scan, detect, and understand all the software or code entering a system, including runtimes, open-source code, and operating systems. Organizations need to detect, identify, analyze, and mitigate all software from third parties and software vendors.

4. The AI Question

There was a lot of discussion around the impact of AI and machine learning on cybersecurity at the RSAC 2023. As is typical in the cyber market, AI can be used both for and against security. Just as AI/ML technologies are increasingly used in real-time analysis and threat hunting, they can be used to create new attacks and breaches.

The new boom in generative AI can make things more fluid for both the good guys and the bad guys. On the solutions front, AI/ML tools can streamline tasks such as responding to queries and alerts and responding to escalating incidents. On the side of the bad guys, generative AI will create new social engineering attacks as well as compliance headaches for CxOs trying to keep their secrets and code secure.

"Detecting the API connections to OpenAI is something you should be thinking about," Wib's Herrin told us. "It's not just shadow API of which you are unaware, it's also outbound calls."

This is likely to boost demand for new tools that address API and code security, because AI/ML often starts with a new API call.

A couple AI/ML-related news stories stuck out:

- HiddenLayer, another company to watch, was named Most Innovative Startup in the RSAC Innovation Sandbox contest. HiddenLayer is an AI application security company based out of Austin, Texas, that has a patent-pending solution to monitor ML algorithms for adversarial attack techniques. It was selected by a panel for helping enterprises safeguard the ML models behind their critical products with a comprehensive security platform, according to the statement from the panel (see more in the Companies to Watch section).

- SentinelOne said its AI threat-hunting can deliver real-time, autonomous response to attacks. Using embedded neural networks and a large language model (LLM)-based interface enables security teams to ask complex threat- and adversary-hunting questions and run operational commands to manage their entire enterprise environment using natural language.

AI/ML is likely to have a huge impact on cybersecurity platforms going forward, both from the risk and solutions standpoint.

United States officials recently issued specific statements of concern.

"There is a wide breadth of risks plus benefits with AI," said Eric Goldstein, Executive Assistant Director for Cybersecurity at the U.S. Cybersecurity and Infrastructure Security Agency, in an interview with the *Wall Street Journal* at the RSAC.

We'll see an acceleration of this activity in the next 12 months, as vendors integrate AI tools with their cybersecurity platforms to more quickly analyze data and stay a step ahead of attacks.

5. Appendix: Shift left and API Security Companies to Watch

[Editor's note: This Companies to Watch section is not an exhaustive list, but a collection of shift left, API, and AI security companies that Futuriom believes are particularly relevant to the market. Futuriom does not require sponsorship to be included on this list. Some of these companies were included in our Futuriom 50 list of top cloud infrastructure startups.]

Akamai

https://www.akamai.com

Cambridge, Mass.-based Akamai Technologies was founded in 1998 and has a 20-plus-year history providing Web and mobile performance acceleration products, content delivery networks, and security solutions. Akamai has been making a big push into cybersecurity with two business units, Security Technology and Edge Technology, to help it better align the company with security and edge technology solutions. Akamai's security offerings include products and services focused on providing secure access, threat protection, zero trust, anti-malware and anti-phishing, and DNS security and anti-DDoS. Akamai recently extended its security platform into API security with the acquisition of Neosec, a pure play delivering API security. Akamai is public and trades on the Nasdaq under symbol AKAM.

Cequence

https://www.cequence.ai/

The Cequence Unified API Protection (UAP) solution provides runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against ever evolving online attacks. Cequence focuses on mitigating cybersecurity risks across all phases of the API security lifecycle -- including, discovery, inventory, compliance, detection, protection, and testing. Based in Sunnyvale, Calif., Cequence was founded by CEO Ameya Talwalkar and CTO Shreyans Mehta. It has raised a total of $100 million from investors including Menlo Ventures, ICON Ventures, Telstra Ventures, HarbourVest Partners. Shasta Ventures, Dell Technologies Capital, and T-Mobile Ventures.

HiddenLayer

https://hiddenlayer.com/

HiddenLayer aims to protect ML from inference, bypass, extraction attacks, and model theft while analyzing the behavior of in-production models with a cloud-based software solution and light-touch consulting. HiddenLayer's patent-pending solution provides a software-based platform that monitors the inputs and outputs of machine-learning algorithms for anomalous activity consistent with adversarial ML attack techniques. Based in Austin, Texas, HiddenLayer has raised $6 million in funding from Ten Eleven Ventures and Secure Octane. It was founded by CEO Christopher Sestito, Chief Scientist Tanner Burns, and CTO Jim Ballard.

Noname Security

https://nonamesecurity.com/

Noname Security automatically discovers APIs, domains, and issues. It can take inventory of every type of API, including HTTP, RESTful, GraphQL, SOAP, XML-RPC, and JSON-RPC; it can also be used to discover legacy and rogue APIs not managed by an API gateway, and catalog data type classifications for all APIs. Noname finds exploitable intelligence, such as leaked information, to understand the attack paths available to potential adversaries. Based in Palo Alto, Calif., the company was founded by CEO Oz Golan and CTO Shay Levi. It has raised $220 million in total funding from investors including Georgian, Lightspeed, Insight Partners, Cyberstarts, Next47, Forgepoint, and the Syndicate Group.

Orca Security

https://orca.security/

Orca Security delivers a single SaaS-based cloud security platform for workload and data protection, cloud security posture management, vulnerability management, and compliance management. The solution delivers security and compliance for AWS, Azure, Google Cloud Platform, and Alibaba Cloud, without the operational costs of agents. Orca's SideScanning allows customers to achieve complete visibility and coverage without sending a single packet over the network or running a single line of code in their environment. Based in Portland,

Oregon, Orca was founded by Avi Shua, Gil Geron (CEO), Liran Antebi, and Matan Ben Gur. It has raised $630 million in funding from investors including Investors include Temasek, CapitalG (Alphabet's independent growth fund), Redpoint Ventures, GGV, ICONIQ Capital, Lone Pine Capital, Stripes, Adams Street Partners, Willoughby Capital, and Harmony Partners.

Salt Security

https://salt.security/

The Salt Security platform collects API traffic across the entire application landscape and makes use of AI/ML and a cloud-scale API data lake to discover all APIs and their exposed data, stop attacks, and eliminate API vulnerabilities with remediation insights learned during runtime. The platform learns the behavior of a company's APIs and requires no configuration or customization to pinpoint and block API attackers. The company was founded in 2018 and led by co-founder and CEO Roey Eliyahu and by co-founder & COO Michael Nicosia. It has raised a total of $270 million from investors including Sequoia, DFJ Growth, and Y Combinator.

Wib

https://wib.com/

Wib is a fast-growth API security startup on a mission to secure the APIs that power today's modern business economy. Wib's holistic API security platform provides continuous and complete visibility and control across the entire API lifecycle – code, testing and production – to help unify DevSecOps teams by providing one single view of the entire API landscape. Wib's unique and pioneering API security approach enables organizations to deliver rigorous real-time inspection, management, and control at every stage of the API lifecycle; automate inventory and API change management; identify rogue, zombie and shadow APIs; and analyze business risk and impact to help reduce and harden their API attack surface. Based in Tel Aviv, Israel, Wib was founded in 2021 by Gil Don, Ran Ohayon, Tal Steinherz and has raised $16 million from investors including Kmehin Ventures, Koch Disruptive Technologies, TechStars, and Venture Israel.